

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. **(Currently Amended)** A system comprising a trusted computing platform including:

at least one first logically protected computing compartment associated with initialization of said system,

and

at least one second logically protected computing compartment, each second logically protected computing compartment being associated with at least one service or process supported by said system,

wherein the system is arranged to load onto said trusted computing platform a predetermined security policy including at least one security rule for controlling the operation of each of said logically protected computing ~~environments~~ compartments;

wherein the security rule relating to the at least one first logically protected computing compartment is arranged to be loaded onto said trusted computing platform when the system is initialized, and

wherein the at least one security rule relating to the at least one second logically protected computing compartment is only arranged to be loaded onto said trusted computing platform if one or more services or processes associated therewith are enabled.

2. **(Previously Presented)** A system according to claim 1, wherein one or more common variable is defined for each compartment, wherein a relevant security rule is only arranged to be added if the variable associated with a particular compartment is enabled.

3. (Previously Presented) A system according to claim 2, wherein at least one variable associated with a directory of plug-ins is arranged to be added.
4. (Previously Presented) A system according to claim 3, wherein the system is arranged to determine, in response to a compartment being enabled, a status of said at least one variable and cause a relevant plug-in based upon the directory of plug-ins to run only if an associated variable is 'true'.
5. (Previously Presented) A system according to claim 4, wherein the at least one compartment includes an operating system compartment arranged to be controlled by the operating system kernel.
6. (Previously Presented) A system according to claim 5, wherein the at least one compartment and network resources are arranged so communication between them is provided via relatively narrow kernel level controlled interfaces to a transport mechanism.
7. (Previously Presented) A system according to claim 6, wherein said communication is governed by rules specified on a compartment by compartment basis.
8. (Previously Presented) A system according to claim 7, including means for determining when a service is starting, and on being enabled, for loading the compartment associated with that service and loading the at least one security rule associated with that service.
9. (Previously Presented) A system according to claim 8, including means for determining when a service starts, and causing the at least one security rule to be loaded accordingly.

10. (Previously Presented) A system according to claim 1, wherein the at least one compartment includes an operating system compartment arranged to be controlled by the operating system kernel.

11. (Original) A system according to claim 1, including means for determining when a service is starting, and on being enabled, for loading the compartment associated with that service and loading the security rules associated with that service.

12. **(Currently Amended)** A method of loading a security policy onto a system including a trusted computing platform, said trusted computing platform including at least one first logically protected computing ~~environments~~ compartments associated with initialization of said system, and at least one second logically protected computing compartments, the at least one second logically protected computing compartments being associated with at least one service or process supported by said system, said security policy comprising one or more security rules for controlling the operation of said the at least one logically protected computing compartments, the method including the steps of:

loading said security rules relating to the at least one first logically protected computing ~~environment~~ compartments onto said trusted computing platform when the system is initialized, and

loading the at least one security rule relating to the at least one second logically protected computing compartments onto said trusted computing platform only if one or more services or processes associated therewith are enabled.